Docket No. 248109US2RD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Fumihiko IKEGAMI, et al. GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: SYSTEM AND APPARATUS FOR INFORMATION DISPLAY

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-047122	February 25, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Katherine D. Pauley

Eckhard H. Kuesters
Registration No. 28,870

Katherine D. Pauley
Registration No. 50,607

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月２５日

出願番号
Application Number: 特願２００３－０４７１２２

[ST. 10/C]: [ＪＰ２００３－０４７１２２]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７５１４

【書類名】　特許願
【整理番号】　13985701
【提出日】　平成15年 2月25日
【あて先】　特許庁長官殿
【国際特許分類】　C06F　3/14
【発明の名称】　情報表示装置、情報表示方法および情報表示システム
【請求項の数】　18
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　池　上　史　彦
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　村　井　信　哉
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　山　口　尚　吾
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　堀　口　健　生
【特許出願人】
【識別番号】　000003078
【住所又は居所】　東京都港区芝浦一丁目１番１号
【氏名又は名称】　株式会社　東　芝

【代理人】
　【識別番号】　100075812
　【弁理士】
　【氏名又は名称】　吉　武　賢　次
【選任した代理人】
　【識別番号】　100088889
　【弁理士】
　【氏名又は名称】　橘　谷　英　俊
【選任した代理人】
　【識別番号】　100082991
　【弁理士】
　【氏名又は名称】　佐　藤　泰　和
【選任した代理人】
　【識別番号】　100096921
　【弁理士】
　【氏名又は名称】　吉　元　弘
【選任した代理人】
　【識別番号】　100103263
　【弁理士】
　【氏名又は名称】　川　崎　康
【手数料の表示】
　【予納台帳番号】　087654
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報表示装置、情報表示方法および情報表示システム

【特許請求の範囲】

【請求項１】

通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、

前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、

前記鍵情報を配布するために表示する鍵情報表示手段と、

前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信する認証情報受信手段と、

前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、

前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、

前記鍵情報の配布範囲を、前記鍵情報表示手段の表示を見ることができる範囲にすることで、前記通信装置を限定することを特徴とする情報表示装置。

【請求項２】

前記鍵情報表示手段は、表示する前記鍵情報を、前記情報表示手段により表示可能な映像に変換し、前記情報表示手段が表示する表示情報の画像と重ねて表示することを特徴とする、請求項１に記載の情報表示装置。

【請求項３】

画面表示手段をさらに備え、

前記鍵情報表示手段は、表示する前記鍵情報を、前記画面表示手段に文字または画像として表示することを特徴とする請求項１に記載の情報表示装置。

【請求項４】

通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、

前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、

前記鍵情報を配布するために音声出力する鍵情報出力手段と、

前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信する認証情報受信手段と、

前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、

前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、

前記鍵情報の配布範囲を前記鍵情報出力手段が発する音声を聞くことができる範囲にすることで、前記通信装置を限定することを特徴とする情報表示装置。

【請求項５】

通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、

前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、

前記鍵情報を配布するために赤外線通信により送信する鍵情報送信手段と、

前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信する認証情報受信手段と、

前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、

前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、

前記鍵情報の配布範囲を、前記鍵情報送信手段が送信する赤外線を受信することができる範囲にすることで、前記通信装置を限定することを特徴とする情報表示装置。

【請求項６】

前記認証手段で認証した通信装置に、前記情報表示手段が表示している表示情報を送信する表示情報送信手段をさらに備えたことを特徴とする、請求項１、４及び５のいずれかに記載の情報表示装置。

【請求項７】

前記表示情報受信手段は、前記鍵情報生成手段が新たに鍵情報を生成しない限り、前記認証手段が一度認証した通信装置ついては都度前記認証手段の認証を得

ることなく、この通信装置から表示情報を受信することを特徴とする請求項１、４及び５のいずれかに記載の情報表示装置。

【請求項８】

前記認証情報及び前記表示情報の通信に利用する通信方式と、前記鍵情報の配布に利用する通信方式とは異なる通信方式であることを特徴とする請求項１、４、５及び６のいずれかに記載の情報表示装置。

【請求項９】

前記表示情報送信手段は、送信する表示情報を前記通信装置で復号可能に暗号化することを特徴とする請求項６に記載の情報表示装置。

【請求項１０】

通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置において、

前記通信装置を認証するための鍵情報を生成し、

前記鍵情報を配布するために出力し、

前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信し、

前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証し、

前記認証した通信装置の表示情報を、表示すべき表示情報として受信することにより、

前記鍵情報の配布範囲を、前記出力を得ることができる範囲に制限することで、前記通信装置を限定することを特徴とする情報表示方法。

【請求項１１】

前記出力は、表示、音声または赤外線のいずれかの伝達方式を用いることを特徴とする請求項１０に記載の情報表示方法。

【請求項１２】

通信装置と、該通信装置から送信した表示情報を受信して表示する情報表示手段を備えた情報表示装置を有する情報表示システムであって、

前記通信装置は、

前記情報表示装置が出力した鍵情報を入力するための鍵情報入力手段と、

前記鍵情報を用いて、前記通信装置を認証するための認証情報を生成する認証情報生成手段とを備え、

前記情報表示装置は、

前記鍵情報を生成する鍵情報生成手段と、

前記鍵情報を配布するために出力する鍵情報出力手段と、

前記認証情報を受信する認証情報受信手段と、

前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、

前記認証した前記通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、

前記鍵情報の配布範囲を、前記鍵情報出力手段の出力を受け取ることができる範囲に制限することで、前記通信装置を限定することを特徴とする情報表示システム。

【請求項１３】

前記情報表示装置は、前記認証手段で認証した通信装置に、表示している表示情報を送信する表示情報送信手段をさらに備えたことを特徴とする、請求項１２に記載の情報表示システム。

【請求項１４】

前記鍵情報の出力は、表示、音声または赤外線のいずれかの伝達方式を用いて行うことを特徴とする請求項１２に記載の情報表示方法。

【請求項１５】

前記鍵情報出力手段は、出力する前記鍵情報を、前記情報表示手段により表示可能な映像に変換し、前記情報表示手段が表示する表示情報の画像と重ねて表示することを特徴とする、請求項１２に記載の情報表示システム。

【請求項１６】

前記鍵情報入力手段は、前記鍵情報出力手段が出力した鍵情報を撮像するカメラを備えていることを特徴とする請求項１５に記載の情報表示システム。

【請求項１７】

前記通信装置は、表示情報を前記情報表示装置で復号化可能に暗号化する暗号化手段を備え、送信する表示情報を暗号化して送信することを特徴とする請求項１２に記載の情報表示システム。

【請求項１８】

前記通信装置は、表示情報を前記情報表示装置で復号化可能に暗号化する暗号化手段を備え、前記情報表示装置に送信する表示情報を暗号化し、前記情報表示装置は、前記表示情報送信手段により送信する表示情報を前記通信装置が復号可能に暗号化することを特徴とする請求項１３に記載の情報表示システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は情報表示装置、情報表示方法および情報表示システムに関する。

【０００２】

【従来の技術】

ノートＰＣやＰＤＡ等の携帯可能な通信装置が普及している。近年、会議またはイベントの参加者は、自己の通信装置を会議またはイベントに持参し、これらの通信装置を通して発表等を行うことが一般的になってきている。

【０００３】

例えば、会議またはイベントの発表者は、自己の通信装置に発表用の資料を電子データとして予め格納しておき、発表の際に、通信装置内の電子データをプロジェクタ、テレビ、モニタ、スピーカ等の情報出力装置を通じて出力する。

【０００４】

このような場合、従来、発表者の通信装置と情報出力装置とはシリアルケーブルやビデオケーブル等のケーブルで接続されるのが一般的であった。

【０００５】

近年、無線の通信装置が普及してきたために、発表者の通信装置と情報出力装置とが無線で接続されるケースが増加してきた。発表者の通信装置と情報出力装置とが無線で接続された場合には、ケーブルを接続する手間が不要であることや参加者の通信装置の場所に制約がないこと等の利点を有する。

【０００６】

しかし、悪意のある第三者が、情報出力装置に接続することによって故意に発表の進行を妨害する、あるいは、発表者の通信装置と情報出力装置との間で送受信されているデータを不正に取得するおそれがある。このように、発表者の通信装置と情報出力装置とが無線で接続された場合には、それらをケーブルで接続した場合には生じ得ないセキュリティ上の問題が生じてしまう。

【０００７】

【特許文献１】

特開２００２－２１８４２０公報

【０００８】

【発明が解決しようとする課題】

この問題の対策として、発表者の通信装置と情報出力装置との間で送受信されるデータを暗号化することが考えられる。例えば、会議またはイベント（以下、会議等という）に参加を許可された者に暗号鍵を事前に配布する。

【０００９】

会議等の開催現場において、暗号鍵を有する参加者は、発表者として通信装置を介してデータを暗号化して情報出力装置へ送信することができ、情報出力装置は、このデータを複合化して出力することができる。また、暗号鍵を有する参加者は、暗号鍵によって、発表者が送信したデータを各自の通信装置により複合化し、その発表の内容を見る、または、聞くことができる。

【００１０】

しかし、事前に暗号鍵を配布することによって、暗号鍵が参加を許可された者の以外の者に渡る可能性がある。また、参加を許可された者であっても、暗号鍵を忘れてしまったような場合には、発表すること、発表の内容を見ること、または、発表の内容を聞くことができなくなってしまう。事前に暗号鍵を配布することは、このような不利益の原因となる。

【００１１】

特許文献１に記載されている技術は、善意の第三者が誤って関係のない情報出力装置にデータを送ってしまうことによって、他人のプレゼンテーションや不用

意に会議の進行を妨害してしまうことを、防止することができる。例えば、参加者が自己の通信装置に出力したい情報出力装置の識別情報を入力する方法が考えられる。この通信装置は、情報出力装置から出力したい画像情報と共にこの入力した識別情報を出力したい情報出力装置へ送信する。この情報出力装置は、受信した識別情報が自己の識別情報と一致したときに限り受信した画像情報を出力する。

【００１２】

この技術によれば、善意の第三者が誤って関係の無い情報出力装置に接続してしまうことを防止することはできる。しかし、識別情報は、暗号化等により保護されることなくそのまま送られるので、盗聴等により無関係の人間にも容易に知られてしまう可能性がある。従って、悪意のある隠れた第三者がいた場合には、この第三者による妨害を防止することはできない。

【００１３】

ところで、会議等においては、参加者全員が互いに顔見知りである場合が多い。また、参加者の中に知り合いでない者がいる場合であっても、デジタル証明などの証明手段あるいは身分証などにより参加者の身分を確認することができることも多い。このような場合には、会議等の会場内にいる不審者を見つけ出し、その会場内から退去させることも可能である。

【００１４】

そこで、本発明の目的は、会議等の会場にいる者はその会議等への参加を許可された者であるという前提のもと、参加者以外の第三者による発表の妨害を防止するとともに、参加者以外の第三者による発表内容の盗取を防止する情報出力装置、情報出力システムおよび情報出力方法を提供することである。

【００１５】

【課題を解決するための手段】

本発明に従った実施の形態による情報表示装置は、通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を配布するために表示する鍵情報表示手段と、前記通信装置が該鍵情報を受け取ったことを認証

するための認証情報を受信する認証情報受信手段と、前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、前記鍵情報の配布範囲を、前記鍵情報表示手段の表示を見ることができる範囲にすることで、前記通信装置を限定する。

【００１６】

本発明に従った実施の形態による情報表示装置は、通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を配布するために音声出力する鍵情報出力手段と、前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信する認証情報受信手段と、前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、前記鍵情報の配布範囲を前記鍵情報出力手段が発する音声を聞くことができる範囲にすることで、前記通信装置を限定する。

【００１７】

本発明に従った実施の形態による情報表示装置は、通信装置から受信した表示情報を表示する、情報表示手段を備えた情報表示装置であって、前記通信装置を認証するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を配布するために赤外線通信により送信する鍵情報送信手段と、前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信する認証情報受信手段と、前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、前記認証した通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、前記鍵情報の配布範囲を、前記鍵情報送信手段が送信する赤外線を受信することができる範囲にすることで、前記通信装置を限定する。

【００１８】

本発明に従った実施の形態による情報表示方法は、通信装置から受信した表示

情報を表示する、情報表示手段を備えた情報表示装置において、前記通信装置を認証するための鍵情報を生成し、前記鍵情報を配布するために出力し、前記通信装置が該鍵情報を受け取ったことを認証するための認証情報を受信し、前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証し、前記認証した通信装置の表示情報を、表示すべき表示情報として受信することにより、前記鍵情報の配布範囲を、前記出力を得ることができる範囲に制限することで、前記通信装置を限定する。

【００１９】

本発明に従った実施の形態による情報表示システムは、通信装置と、該通信装置から送信した表示情報を受信して表示する情報表示手段を備えた情報表示装置を有する情報表示システムであって、

前記通信装置は、前記情報表示装置が出力した鍵情報を入力するための鍵情報入力手段と、前記鍵情報を用いて、前記通信装置を認証するための認証情報を生成する認証情報生成手段とを備え、

前記情報表示装置は、前記鍵情報を生成する鍵情報生成手段と、前記鍵情報を配布するために出力する鍵情報出力手段と、前記認証情報を受信する認証情報受信手段と、前記認証情報が前記鍵情報に基づいて作成されたものかどうかを検証することで前記通信装置を認証する認証手段と、前記認証した前記通信装置の表示情報を、表示すべき表示情報として受信する表示情報受信手段とを備え、

前記鍵情報の配布範囲を、前記鍵情報出力手段の出力を受け取ることができる範囲に制限することで、前記通信装置を限定する。

【００２０】

【発明の実施の形態】

以下、図面を参照し、本発明による実施の形態を説明する。実施の形態は本発明を限定するものではない。

【００２１】

本発明による実施の形態において、会議等の各参加者は通信機能を有するノートＰＣ（Personal Computer）やＰＤＡ（Personal Data Assistants）などの通信装置を持ち寄る。参加者のうち発表者は、自己の通信装置に格納された電子的な

プレゼンテーション用のデータをプロジェクタ、テレビ、モニタ、スピーカ等の情報出力装置へ送信し、情報出力装置にこのデータを表示させる。ここでいう表示とは画像、音声、文字、その他の情報全般を、その場に居合わせた参加者に示すことを指す。このような電子的なプレゼンテーションにおいて、情報出力装置は、データの表示を許可するか、若しくは、却下するかの認証処理を行う。

【００２２】

（第1の実施形態）

図１（Ａ）は、本発明に係る実施の形態に従った情報出力装置１００のブロック図である。情報出力装置１００は、秘密情報生成部１０、秘密情報出力部２０、送受信部３０、認証処理部４０およびデータ出力部５０を備えている。本実施の形態において、情報出力装置１００は、データ出力部５０によって画像をスクリーン（図示せず）に投影して出力するプロジェクタ等である。

【００２３】

図１（Ｂ）は、図１（Ａ）に示した情報出力装置１００と無線で通信することができる通信装置１０１のブロック図である。通信装置１０１は、秘密情報取得部６０、認証情報生成部７０、送受信部８０およびデータ記憶部９０を備えている。本実施の形態において、通信装置１０１は、情報出力装置１００と無線で通信可能に接続されたＰＣやＰＤＡ等である。

【００２４】

秘密情報生成部１０は秘密情報を生成する。秘密情報は、例えば、文字、数字、記号、図形のいずれかでよく、これらの組合せでもよい。より詳細には、文字、数字および記号を配列した“RFYOHR#104”のような文字列であってもよい。円、多角形、バーコード等の図形のであってもよい。

【００２５】

秘密情報生成部１０は、秘密情報としてランダムな値を生成する乱数発生器でもよく、予め設定されたアルゴリズムにより秘密情報を生成する装置でもよい。尚、アルゴリズムにより秘密情報を生成する場合には、アルゴリズム自体またはアルゴリズムに用いられるパラメータが秘密にされていなければならない。アルゴリズム自体またはアルゴリズムに用いられるパラメータが知られると、以前の

秘密情報から今回の秘密情報を推測され得るからである。

【００２６】

秘密情報生成部１０は、情報出力装置１００の起動時に秘密情報を自動的に生成する。しかし、会議等の参加者または主催者の指示により秘密情報を生成してもよい。例えば、情報出力装置１００に秘密情報の生成を指示するボタンを設ける。秘密情報生成部１０は、参加者または主催者がこのボタンを押したときに秘密情報を生成する。さらに、このようなボタンを複数設けることによって、秘密情報生成部１０は、いずれのボタンが選択されたかに基づいて秘密情報を生成し、若しくは、押されたボタンの順番に基づいて秘密情報を生成することができる。

【００２７】

秘密情報出力部２０は、通信装置１０１または参加者のみに認識可能なように秘密情報を出力する。秘密情報を参加者に対してのみ認識できるように出力するために、情報出力装置１００は、例えば、情報出力装置１００と物理的に近接した範囲のみに秘密情報を出力する。

【００２８】

より詳細には、情報出力装置１００が会議等が開催される部屋の内部に設置され、情報出力装置１００は、秘密情報をスクリーンへ投影する。これにより、部屋の内部にいる参加者のみが秘密情報を得ることができる。この場合、秘密情報出力部２０はプロジェクタの投影部である。情報出力装置１００が設置される場所は会議室などの部屋に限定されるものではなく、持ち運び可能な情報出力装置１００を屋外に設置してもよい。例えば、情報出力装置１００がその近傍にいる参加者のみに対して秘密情報を音声で出力してもよい。この場合、秘密情報出力部２０はスピーカである。

【００２９】

秘密情報出力部２０は、情報出力装置１００の筐体に備えられた小型の液晶ディスプレィであってもよい。この場合には、会議等の主催者または参加者が、液晶ディスプレィに表示された秘密情報を大きく書き写し、あるいは、読み上げることによって、他の参加者に周知させる。

【００３０】

秘密情報出力部２０は、上述の出力手段の複数を組み合せてもよい。例えば、筐体に付けられた小型の液晶ディスプレィに秘密情報を表示すると共に、スピーカから音声として出力してもよい。これにより、参加者に秘密情報を確実に伝えることができる。

【００３１】

秘密情報が参加者以外の第三者に知られるのを防ぐため、秘密情報の出力は、情報出力装置１００の操作者によりコントロールされることが好ましい。例えば、情報出力装置１００の筐体にボタンを設け、操作者がこのボタンを押したときに限り秘密情報が表示されるようにする。操作者がこのボタンを押してから、例えば、１０秒間経過後に自動的に秘密情報が非表示になるようにしてもよい。さらに、操作者がこのボタンを押したときに秘密情報を非表示状態にしてもよい。情報出力装置１００にリモコン装置が付属している場合、操作者はリモコン装置から秘密情報の表示／非表示のコントロールができることが好ましい。

【００３２】

秘密情報取得部６０は、例えば、キーボードやタッチパネル等の入力装置である。この場合、参加者は、秘密情報を知得すると、この秘密情報をキーボードやタッチパネル等に入力する。

【００３３】

秘密情報出力部２０および秘密情報取得部６０は、１会議室内程度の近距離で通信が可能な電波または超音波、赤外線等の無線通信手段で接続された入出力インタフェースであってもよい。この場合、秘密情報出力部２０は、その近傍に存在する通信装置１０１にのみ秘密情報を送信する。これにより、通信装置１０１は、秘密情報出力部２０が出力した秘密情報を、主催者や参加者を介することなく直接取得することができる。

【００３４】

送受信部３０は、通信装置１０１が秘密情報に基づいて生成した認証情報を、通信装置１０１から受信する。認証処理部４０は、秘密情報を用いて認証情報を検証することにより通信装置１０１の認証を行う。認証情報の検証は、例えば、

公開鍵暗号方式または秘密鍵暗号方式を採用する。この場合、認証情報は、秘密情報にデジタル署名を施した情報である。

【００３５】

認証処理部４０により認証された通信装置１０１は情報出力装置１００へ発表情報を送信することを許可される。情報出力装置１００は、認証された通信装置１０１からの発表情報をスクリーンへ投影する。一方で、認証処理部４０により認証されなかった通信装置が情報出力装置１００へ発表情報を送信しても、情報出力装置１００はこの発表情報を受信しない、若しくは、この発表情報をスクリーンへ投影しない。

【００３６】

図１（Ａ）に示した情報出力装置１００は単一の機器で構成されている。しかし、情報出力装置１００は、従来の画像投影機能を有するプロジェクタおよびそのプロジェクタに接続されたＰＣの組合せとして構成することもできる。この場合は、図１（Ａ）に示したデータ出力部５０はプロジェクタに該当し、秘密情報生成部１０および秘密情報出力部２０はＰＣにおいて動作するソフトウェアに該当し、送受信部３０はＰＣに備えられた無線通信用の装置に該当する。

【００３７】

このように、本実施の形態によれば、会議室等の部屋内にいる参加者または情報出力装置１００の近傍にいる者は容易に秘密情報を知ることができる。しかしそれ以外の第三者は秘密情報を知ることができない。従って、会議等の参加者のみが情報出力装置１００へ情報を送信することができる。一方で、会議等に参加していない第三者は情報出力装置１００へ情報を送信することができない。よって、第三者が故意または過失により参加者の発表を妨げることがない。従って、本実施の形態は、外部から妨害されないようにセキュリティが確保されたプレゼンテーションや会議を実現することができる。

【００３８】

図１（Ａ）、図１（Ｂ）および図２を参照して、本実施の形態による情報出力装置１００および通信装置１０１の動作を説明する。

【００３９】

図２は、情報出力装置１００および参加者の通信装置１０１の動作およびこれらの装置間の通信処理を示すフロー図である。情報出力装置１００を起動すると、まず、秘密情報生成部１０が秘密情報を生成する（Ｓ１０）。

【００４０】

秘密情報は、認証処理部４０に送られ記憶されるとともに、秘密情報出力部２０へ送信される（Ｓ２０）。

【００４１】

次に、秘密情報出力部２０が、参加者のみが認識できるように秘密情報を出力する（Ｓ３０）。例えば、会議等の参加者のみが秘密情報を得ることができるように、秘密情報出力部２０は、会議等が開催される室内で秘密情報をスクリーンへ投影する。また、秘密情報出力部２０がスピーカである場合には、秘密情報を参加者のみに聞こえるように音声で出力する。さらに、秘密情報出力部２０が小型の液晶ディスプレイである場合には、会議等の主催者または参加者が、ディスプレィに表示された秘密情報を読み取り、参加者が見ることができるホワイトボード等に書き写す。参加者が秘密情報を読み取ったことを確認した上で秘密情報を消去することにより、参加者のみに秘密情報を周知させることができる。

【００４２】

続いて、認証方法について説明する。

参加者は、秘密情報を知得すると、各自の通信装置１０１にその秘密情報を入力する（Ｓ４１）。例えば、参加者はキーボードやタッチパネル等の秘密情報取得部６０に秘密情報を打ち込む。

【００４３】

秘密情報出力部２０および秘密情報取得部６０が無線通信手段で接続された入出力インタフェースである場合には、秘密情報の送受信は自動で行われるので、参加者は秘密情報を入力する必要はない。この場合、情報出力装置１００は、秘密情報が会議室内部等の限られた範囲のみに届くように、出力を制御しつつ秘密情報を送信する。

【００４４】

認証情報生成部７０は、秘密情報に基づいて認証情報を生成する（Ｓ５１）。

送受信部８０が、認証情報を情報出力装置１００へ送信する（Ｓ６１）。情報出力装置１００の送受信部３０が認証情報を受信する（Ｓ７０）。認証処理部４０が、認証情報を秘密情報に基づいて検証する（Ｓ８０）。

【００４５】

ステップＳ５１からステップＳ８０までは、例えば、公開鍵暗号方式または秘密鍵暗号方式を用いることによって実施することができる。

【００４６】

公開鍵暗号方式を用いた方法は次のようになる。情報出力装置１００は予め参加者の公開鍵を有し、通信装置１０１は予め参加者の秘密鍵を有する。ステップＳ５１において、認証情報生成部７０は、秘密情報に各自の秘密鍵でデジタル署名を施すことによって認証情報を生成する。ステップＳ６１において、通信装置１０１はこのデジタル署名を付した秘密情報を認証情報として情報出力装置１００へ送信する。ステップＳ７０において、情報出力装置１００は認証情報を受信する。ステップＳ８０において、認証処理部４０が、その認証情報を送信した通信装置の所有者の公開鍵によってデジタル署名を確認する。これにより、正当な参加者の秘密鍵が通信装置１０１に格納されていることが確認され得る。さらに、デジタル署名が施された秘密情報の内容を確認することによって、通信装置１０１の所有者が秘密情報を知っていることが確認され得る。

【００４７】

秘密鍵暗号方式を用いた方法は次のようになる。情報出力装置１００および通信装置１０１が参加者の秘密鍵を予め有する。ステップＳ５１において、認証情報生成部７０は、秘密情報を各自の秘密鍵で暗号化することによって認証情報を生成する。ステップＳ６１において、通信装置１０１はこの暗号化された秘密情報を認証情報として情報出力装置１００へ送信する。ステップＳ７０において、情報出力装置１００は認証情報を受信する。ステップＳ８０において、認証処理部４０が、その認証情報を送信した参加者の秘密鍵で復号化する。復号化した認証情報と秘密情報生成部１０において生成した秘密情報とが同じである場合に、その認証情報を送信した者が正当な参加者であると判断する。

【００４８】

但し、複数の参加者が秘密鍵を共有する場合には、秘密情報を知らない一の共有者が他の共有者により送信された認証情報を傍受し、その認証情報を自己の認証情報として送信することが可能となる。この場合、情報出力装置１００は、秘密情報を知らない者を誤って正当な参加者と判断してしまう。従って、秘密鍵は参加者ごとに異なることが必要である。

【００４９】

尚、秘密鍵は、時間の経過と共に変更されるように設定してもよい。例えば、秘密鍵は、情報出力装置１００と通信装置１０１との間の共通のアルゴリズムに基づき同期して変更されてもよい。

【００５０】

公開鍵暗号方式または秘密鍵暗号方式は、認証処理において通信装置１０１と情報出力装置１００との間の通信を簡略化することができる。即ち、図２の矢印が示すように、通信装置１０１は、認証情報を情報出力装置１００へ送信するだけで足り、その他の通信を必要としない。情報出力装置１００から通信装置１０１への通信も必要としない。これにより、認証処理における通信が簡略化されるだけでなく、情報出力装置１００の送受信部３０が送信機能を必要としなくなる。即ち、送受信部３０は受信部３０でよい。また、通信装置１０１の送受信部８０が受信機能を必要としなくなる。即ち、送受信部８０は送信部８０でよい。

【００５１】

公開鍵暗号方式または秘密鍵暗号方式は、情報出力装置１００に予め参加者の公開鍵または秘密鍵を格納しておかなければならないので、事前の設定に手間がかかるという問題がある。この問題を解決するためには、いわゆるチャレンジ・レスポンス方式を用いることによって解決することができる。尚、チャレンジ・レスポンス方式を用いる場合には、送受信部３０は送信機能を必要とし、送受信部８０は受信機能を必要とする。

【００５２】

より詳細には、まず、情報出力装置１００は、通信装置１０１のそれぞれに対して個別のランダム値をチャレンジとして送信する。通信装置１０１は、秘密情報を暗号鍵としてこのランダム値を暗号化し、さらに、この暗号化されたランダ

ム値をレスポンスとして情報出力装置１００へ返信する。情報出力装置１００は秘密情報を暗号鍵としてレスポンスを複号化する。その結果、レスポンスを複合化して得られた値がチャレンジとして送信したランダム値と同一である場合に、通信装置１０１が正当であると認証する。このようなチャレンジ・レスポンス方式によって、情報出力装置１００は、予め各参加者の公開鍵または秘密鍵を格納する必要がなくなる。

【００５３】

尚、上述の認証方法はあくまでも例示的なものであり、他の認証方法を用いてもよい。情報出力装置１００は、その認証方法によって同一の秘密情報を通信装置１０１が有していることを確認できればよい。

【００５４】

次に、通信装置１０１が情報出力装置１００へコネクション設立の許可を求める（Ｓ９１）。情報出力装置１００は、認証情報の検証結果に基づいて、コネクションの許可または不許可を判断する（Ｓ１００）。即ち、情報出力装置１００は、コネクションを求める通信装置１０１の所有者が正当な参加者である場合にはコネクションを許可し、一方で、その所有者が正当な参加者以外の第三者である場合にはコネクションを却下する。

【００５５】

通信装置１０１の所有者が正当な参加者であると認証された場合、通信装置１０１は、プレゼンテーション用の資料を情報出力装置１００へ送信する（Ｓ１２１）。このとき、秘密情報に基づいた暗号鍵でプレゼンテーション用のデータを暗号化する。それにより、秘密情報を知らない第三者がプレゼンテーション用の資料を盗取することを防止できる。情報出力装置１００は、通信装置１０１からのプレゼンテーション用の資料をデータ出力部５０からスクリーンに投影する（Ｓ１３０）。尚、ステップＳ１００の後、情報出力装置１００は、正当な参加者の通信装置１０１へコネクションの許可を通知してもよい。この場合、ステップＳ１２１において、コネクション許可の通知を受けた通信装置１０１が、プレゼンテーション用の資料を情報出力装置１００へ送信する。

【００５６】

情報出力装置１００は、秘密情報に基づくことなく、暗号鍵を生成し、この暗号鍵を認証された通信装置１０１に配布してもよい。しかし、情報出力装置１００および通信装置１０１が同一のアルゴリズムを用いて共有の秘密情報から暗号鍵を生成することが好ましい。これにより、暗号鍵を通信装置１０１に改めて配布する必要がなくなるからである。

【００５７】

ステップ８０の検証の結果、認証処理部４０が通信装置１０１の所有者を正当な参加者でないと判断した場合、情報出力装置１００は、単にコネクションを許可しないだけでよい（Ｓ１１０）。この場合、情報出力装置１００は、不正な第三者が室内にいることを液晶ディスプレィへ表示してもよい。さらに、情報出力装置１００は、データ出力部５０を通して不正な第三者が室内にいる旨をスクリーンに投影してもよい。情報出力装置１００がスピーカを備えている場合には、音声により不正な第三者が室内にいる旨をアナウンスしてもよい。このとき、情報出力装置１００は、第三者の通信装置の識別子、例えば、アドレスを併せて表示してもよい。これにより、秘密情報を知らない第三者は、情報出力装置１００へ接続することができない。また、情報出力装置１００を試みた第三者を特定することができる。

【００５８】

本実施の形態によれば、秘密情報は情報出力装置１００の起動時に１回だけ生成される。これにより、会議等の途中から参加する者はその最初からの参加者に秘密情報を教えてもらうことにより参加することができる。一方で、途中で退席した参加者が悪意を持った第三者に秘密情報を教えてしまう可能性がある。この問題を解決するためには、秘密情報を適宜変更する。

【００５９】

例えば、情報出力装置１００に秘密情報の更新を指示するためのボタンを設ける。参加者が大幅に入れ替わった場合に、主催者がそのボタンを押して新たな秘密情報を生成させ、図２に示すステップを経て、プレゼンテーション等が開始される。

【００６０】

秘密情報を変更するために、秘密情報生成部１０にタイマを設け、秘密情報を定期的に変更してもよい。秘密情報の更新には、前回の秘密情報を暗号鍵として新しい秘密情報を暗号化し通信装置１０１へ送信することができる。通信装置１０１は、前回の秘密情報によって新しい秘密情報を自動的に取得できる。これにより、秘密情報が変更された場合であっても、参加者は新しい秘密情報を入力し直す必要がなくなる。

【００６１】

発表者の通信装置１０１が情報出力装置１００とのコネクションを切断した時に秘密情報を変更してもよい。この場合は、プレゼンテーションを終了した発表者が自己の通信装置１０１と情報出力装置１００とのコネクションを切断した時に秘密情報が変更される。秘密情報の更新方法としては、以上に説明した方法を複数組み合せて用いてもよい。

【００６２】

このように秘密情報を更新することにより、途中で退席した参加者が第三者に更新前の秘密情報を教えたとしても、その第三者は、更新後の秘密情報を知らないので、会議等に参加することができない。

【００６３】

本実施の形態において情報出力装置１００は、画像を投影するプロジェクタであるが、本発明の情報出力装置はこれに限られない。即ち、情報出力装置１００が出力する情報は画像に限らず、音声であってもよい。情報出力装置１００が出力する情報は、音声および画像の組合せ、即ち、ビデオ信号であってもよい。さらに、情報出力装置１００は、画像または音声のいずれも出力することなく、単に情報を無線によって周囲の通信装置１０１に送信するものでもよい。この場合、通信装置１０１は、個々のディスプレイにプレゼンテーションの内容等を出力する。

【００６４】

会議等の開始前に、案内のために発表者の名前、演題、発表開始時刻、終了時刻などの情報がスクリーンに投影されていることがある。情報出力装置１００は、これらの情報に重ね合わせて秘密情報を表示してもよい。この場合、図１に示

すデータ出力部５０は、秘密情報出力部２０から秘密情報を読み出し、スクリーンに表示中の情報に重ね合わせて秘密情報を表示する。

【００６５】

図３は、発表者の名前等の情報に重ね合わせて秘密情報を表示するときのフロー図である。図２に示すステップＳ１０およびステップＳ２０を実行した後、秘密情報出力部２０は、データ出力部５０がスクリーンに発表者の名前等の情報を投影しているか否かを判断する（Ｓ２２）。

【００６６】

データ出力部５０がスクリーンに発表者の名前等の情報を投影している場合には、データ出力部５０は、秘密情報を発表者の名前等の情報に重ねて表示する（Ｓ３２）。一方で、データ出力部５０が何も投影していない場合には、データ出力部５０は、秘密情報のみを表示する（Ｓ３４）。さらに、図２に示したステップＳ４１からステップＳ１３０を実行する。

【００６７】

（第２の実施形態）

図４は、本発明に係る第２の実施の形態に従った通信装置２０１のブロック図である。情報出力装置１００は、図１（Ａ）に示すものと同様である。

【００６８】

第２の実施の形態に従った通信装置２０１は、発表者が予め用意したデータを情報出力装置１００に送信するだけでなく、発表者が、プレゼンテーション中にその場で入力したデータをも情報出力装置１００に送ることができる。

【００６９】

通信装置２０１は、図１（Ｂ）に示した通信装置１０１の構成要素の他に、データ入力部９２および送信データ生成部９４をさらに備える。データ入力部９２は、データを通信装置２０１へ入力するために備えられている。送信データ生成部９４は、データ記憶部９０に予め格納されたデータおよびデータ入力部９２に入力されたデータに基づいて情報出力装置１００へ送信するためのデータを生成する。このとき、データ記憶部９０に格納されたデータとデータ入力部９２からのデータとを重ね合わせて情報出力装置１００へ送信してもよい。また、送信デ

ータ生成部９４は、データ記憶部９０またはデータ入力部９２のいずれか一方を選択し、そのデータを情報出力装置１００へ送信してもよい。

【００７０】

例えば、データ入力部９２がマイク等の音声入力装置であり、情報出力装置１００が、画像データおよび音声データの両方を出力する機能を備えた装置、例えば、スピーカを備えたプロジェクタまたはテレビであるとする。通信装置２０１は、データ記憶部９０の画像データとデータ入力部９２に入力された音声データとを情報出力装置１００へ送信する。情報出力装置１００はこれらの画像データおよび音声データをともに出力する。これにより、発表者は、情報出力装置１００に画像データを表示させ、同時に、その説明を音声で出力させることができる。プレゼンテーションを行うことができる。このように、本実施の形態によれば、より効果的なプレゼンテーションを行うことができる。

【００７１】

秘密情報が音声として出力された場合、データ入力部９２がこの音声を自動入力する。認証情報生成部７０は、この音声から秘密情報を認識し、秘密情報に基づいて認証情報を生成する。これにより、参加者は、秘密情報を入力する必要がなくなる。

【００７２】

例えば、データ入力部９２がカメラ等の画像入力装置であるとする。この場合、送信データ生成部９４が、データ記憶部９０に予め格納された画像データと、データ入力部９２により撮像された画像データとを選択することができる。これにより、発表者は、データ記憶部９０に予め格納された画像データとデータ入力部９２により撮像された画像データとを適宜切り替えながらプレゼンテーションを行うことができる。例えば、発表者は、プレゼンテーション中に手書きのイラストなどを作成しつつそれを表示させることができる。

【００７３】

秘密情報が画像として出力された場合、データ入力部９２がこの画像を自動入力する。認証情報生成部７０は、この画像から秘密情報を認識し、秘密情報に基づいて認証情報を生成する。これにより、参加者は、秘密情報を入力する必要が

なくなる。例えば、秘密情報がバーコードである場合、データ入力部９２がバーコードを入力する。認証情報生成部７０は、このバーコードに基づいて認証情報を生成し、送受信部８０がこれを情報出力装置１００へ出力する。情報出力装置１００は、認証情報を複合してバーコードを得、情報出力装置１００に予め格納されたバーコードと照合する。これにより、認証処理が実現される。

【００７４】

例えば、データ入力部９２が画像および音声を入力するビデオカメラであり、データ記憶部９０が画像および音声を記憶するビデオテープであるとする。この場合、データ入力部９２に入力された画像および音声を一旦データ記憶部９０に格納しておくことができる。これをまとめて情報出力装置１００へ送信してもよい。

【００７５】

秘密情報が画像および音声の組合せとして出力された場合、データ入力部９２がこの画像および音声を自動入力する。認証情報生成部７０は、この画像および音声から秘密情報を認識し、秘密情報に基づいて認証情報を生成する。これにより、参加者は、秘密情報を入力する必要がなくなる。

【００７６】

図２に示すステップ８０の検証の結果に基づいて、各通信装置２０１が送信できるデータの内容を制限してもよい。例えば、発表者のみに秘密情報を教え、発表者の通信装置２０１はデータ記憶部に格納された画像データおよびデータ入力部９２から入力された音声データの両方を送信することができる。一方で、他の参加者が所有する通信装置２０１はデータ入力部９２から入力された音声データのみを送信することができる。これにより、情報出力装置１００は、発表者が用意した画像のみを表示することによって、プレゼンテーションを円滑に進行させることができる。尚且つ、総ての参加者が音声を情報出力装置１００へ送信できるので、発表者および参加者が発表内容に関する質疑および応答を行うことができる。

【００７７】

（第３の実施形態）

図５（Ａ）および図５（Ｂ）は、本発明に係る第３の実施の形態に従った情報出力装置３００および通信装置３０１のブロック図である。本実施形態では、情報出力装置３００および通信装置３０１の両方が入力機能を備えている。

【００７８】

情報出力装置３００は、図１に示す情報出力装置１００の構成要素の他に、データ入力部５２をさらに備えている。通信装置３０１は、図１に示す通信装置１０１の構成要素の他に、データ出力部９６をさらに備えている。

【００７９】

例えば、情報出力装置３００は書画カメラ付きプロジェクタである。この場合、情報出力装置３００のデータ出力部５０は画像をスクリーンに投影して出力する投影装置である。情報出力装置３００のデータ入力部５２は画像を撮影して入力する小型の書画カメラである。データ入力部５２は紙に印刷された書類や図面などを撮影することができる。データ入力部５２により撮影された画像はデータ出力部５０によりスクリーンに投影される。情報出力装置３００は、データ出力部５０を通して秘密情報を表示してもよい。

【００８０】

通信装置３０１は、情報出力装置３００と通信可能に接続されている。それにより、通信装置３０１は、データ入力部５２により撮影された画像を受信し、データ出力部９６に表示することができる。データ出力部９６は、例えば、ＰＣの液晶ディスプレィである。これにより、参加者は、情報出力装置３００のデータ出力部５０からスクリーンに映し出された内容を手元で見ることができる。

【００８１】

さらに、通信装置３０１は、この画像をデータ記憶部９０に記録することができる。それにより参加者は、プレゼンテーションの内容を電子データとして持ち帰ることができる。データ記憶部は、例えば、ＰＣのハードディスクである。

【００８２】

（第４の実施形態）

図６は、本発明に係る第４の実施の形態における情報出力装置４００のブロック図である。情報出力装置４００は、図５（Ａ）に示す情報出力装置３００の構

成要素の他に、データ記憶部５４を備えている。データ記憶部５４は、発表者から送信されたプレゼンテーション用のデータやデータ入力部５２によって撮像された画像データを記憶することができる。参加者は、図５（Ｂ）に示す通信装置３０１を用いてデータ記憶部５４からプレゼンテーション用のデータや画像データ等を読み出すことができる。尚、通信装置３０１に代えて、通信装置１０１または２０１を用いてもよい。

【００８３】

これらのデータを読み出すときに、図２に示すフローを用いることによってプレゼンテーション用のデータや画像データ等のセキュリティを確保することができる。例えば、ステップＳ６１において、通信装置３０１が、認証情報を情報出力装置４００へ送信する。次に、ステップＳ７０およびＳ８０において、情報出力装置４００が、認証情報を受信してこの認証情報を検証する。ステップＳ９１において、通信装置３０１が、プレゼンテーション用のデータまたは画像データを取得するために、コネクション設立要求を情報出力装置４００へ行う。ステップＳ１００において、情報出力装置４００が、検証結果に基づいて通信装置３０１からのコネクション設立要求を許可または却下する。

【００８４】

コネクション設立要求が許可された場合、情報出力装置４００は、秘密情報に基づいて、プレゼンテーション用のデータまたは画像データを暗号化し、その暗号化されたデータを通信装置３０１へ送信する。これにより、情報出力装置４００から通信装置３０１へプレゼンテーション用のデータや画像データ等を送信するとき、これらのデータのセキュリティが確保される。

【００８５】

情報出力装置４００と通信装置３０１との間で送受信するデータの種類によって認証処理および暗号化を選択的に実行してもよい。例えば、プレゼンテーション用のデータを送信する場合には、情報出力装置４００は認証処理および暗号化を実行する。一方で、データ入力部５２によって撮影された画像データを送信する場合には、情報出力装置４００は認証処理および暗号化を実行することなくこの画像データを通信装置３０１へ送信する。

【００８６】

さらに、発表者のみが秘密情報を知得していてもよい。これにより、発表者はプレゼンテーション用のデータを情報出力装置４００に送信することができる。また、発表者は他の発表者が用いた資料を情報出力装置４００からダウンロードして持ち帰ることができる。一方で、他の参加者は、情報出力装置４００への送信や情報出力装置４００からのダウンロードをすることができず、データ入力部５２によって撮影された画像を各自の通信装置３０１で見ることができるだけである。このように、本実施の形態によれば、発表者とその他の参加者とを区別することができる。

【００８７】

発表者のみに特定の秘密情報を知得させるために、秘密情報生成部１０は、発表者用の秘密情報１および参加者用の秘密情報２をそれぞれ生成する。例えば、秘密情報１は秘密情報出力部２０として設けられた小型液晶ディスプレイに表示する。これにより、発表者のみが秘密情報１を知ることができる。秘密情報２は、データ出力部５０からスクリーンに投影する。これにより、参加者全員が秘密情報２を知得することができる。

【００８８】

通信装置３０１が秘密情報１を有する場合、情報出力装置４００は、通信装置３０１が情報出力装置４００へデータを送信し、または、通信装置３０１が情報出力装置４００からデータをダウンロードすることを許可する。一方で、通信装置３０１が秘密情報２を有する場合、情報出力装置４００は、通信装置３０１がデータ入力部５２によって撮影された画像データをダウンロードすることのみを許可する。

【００８９】

本実施の形態によれば、発表者以外の参加者がプレゼンテーション用のデータを持ち帰るのを防ぐことができる。発表者以外の参加者が故意または過失によりプレゼンテーションを妨害することを防止できる。

【００９０】

（第５の実施形態）

図７は、本発明に係る第５の実施の形態における通信装置４０１のブロック図である。通信装置４０１は、図５（Ｂ）に示す通信装置３０１の構成要素の他に、認証処理部９８をさらに備えている。通信装置４０１は、発表者用の通信装置である。発表者以外の参加者の通信装置は、通信装置１０１、２０１、３０１、４０１のいずれでもよい。便宜的に、発表者以外の参加者の通信装置を通信装置４０２とする。

【００９１】

認証処理部９８は、通信装置４０２から送信された認証情報を検証し、通信装置４０２が通信装置４０１に接続することを許可または却下する。これにより、秘密情報を有する通信装置４０２は、情報出力装置に接続することなく、通信装置４０１からプレゼンテーション用のデータを直接受信することができる。

【００９２】

例えば、図２に示すフローを参照して、通信装置４０１および通信装置４０２の動作を説明する。図２において、情報出力装置１００に代えて通信装置４０１がステップＳ１０からＳ１００までを実行する。図２において、通信装置１０１に代えて通信装置４０２がステップＳ４１からＳ９１までを実行する。但し、ステップＳ２０において、秘密情報は、認証情報生成部７０および認証処理部９８の両方に記憶される。

【００９３】

ステップＳ１００において、通信装置４０１が通信装置４０２からのコネクション設立要求を許可した場合、通信装置４０２は、通信装置４０１のデータ記憶部９０（図７参照）からプレゼンテーション用のデータをダウンロードすることができる。一方で、ステップＳ１００において、通信装置４０１が通信装置４０２からのコネクション設立要求を却下した場合、通信装置４０２は、通信装置４０１に接続することができないので、プレゼンテーション用のデータをダウンロードすることができない。

【００９４】

これにより秘密情報を知得している参加者のみがプレゼンテーション用のデータを持ち帰ることができ、秘密情報を知得している参加者のみが自己の通信装置

４０２でプレゼンテーション用のデータを見ることができる。

【００９５】

本実施の形態において、送受信される情報はプレゼンテーション用のデータに限らない。例えば、参加者と発表者との間で短いテキストメッセージを相互に送受信する、いわゆるチャットを行うこともできる。このチャットも秘密情報に基づいて暗号化されている。よって、秘密情報を知らない第三者は、発表者と参加者の間でのチャットによる質疑応答を妨害または盗取することができない。

【００９６】

以上の実施の形態において、情報出力装置は、図２に示す認証処理や暗号化を行う「セキュアモード」と、これらのセキュリティ対策を行わない「通常モード」とを含む複数の動作モードを選択できるように構成してもよい。主催者または参加者は、会議等の開催される環境に応じてこれらの動作モードを切り替えることができる。例えば、第三者によるデータの妨害または盗取の可能性が極めて低い環境では、「通常モード」が選択される。第三者によるデータの妨害または盗取の可能性が高い環境では、「セキュアモード」が選択される。

【００９７】

【発明の効果】

本発明による情報出力装置、情報出力システムおよび情報出力方法は、参加者以外の第三者による発表の妨害を防止し、参加者以外の第三者による発表内容の盗取を防止することができる。

【図面の簡単な説明】

【図１】

本発明に係る実施の形態に従った情報出力装置１００および通信装置１０１のブロック図。

【図２】

情報出力装置１００および通信装置１０１の動作およびこれらの装置間の通信処理を示すフロー図。

【図３】

発表者の名前等の情報に重ね合わせて秘密情報を表示するときのフロー図。

【図４】

本発明に係る第２の実施の形態に従った通信装置２０１のブロック図。

【図５】

本発明に係る第３の実施の形態に従った情報出力装置３００および通信装置３０１のブロック図。

【図６】

本発明に係る第４の実施の形態における情報出力装置４００のブロック図。

【図７】

本発明に係る第５の実施の形態における通信装置４０１のブロック図。

【符号の説明】

１００、３００、４００　情報出力装置

１０１、２０１、３０１、４０１　通信装置

１０　秘密情報生成部

２０　秘密情報出力部

３０　送受信部

４０、９８　認証処理部

５０、９６　データ出力部

６０　秘密情報取得部

７０　認証情報生成部

８０　送受信部

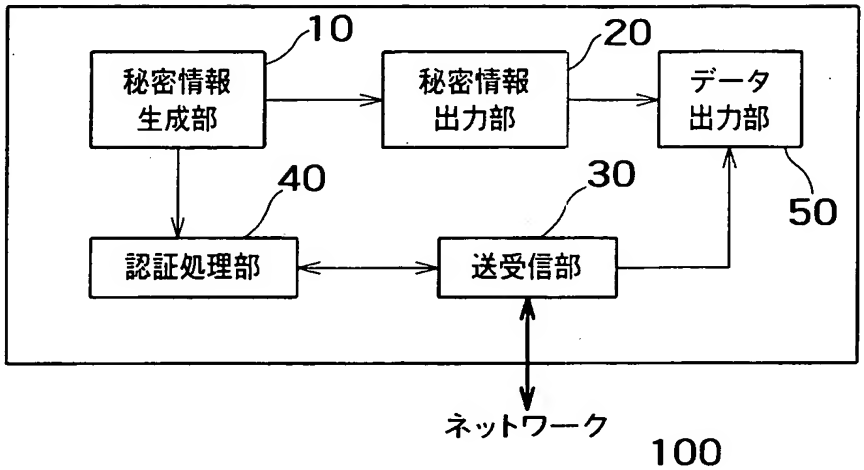
５４、９０　データ記憶部

９２　データ入力部

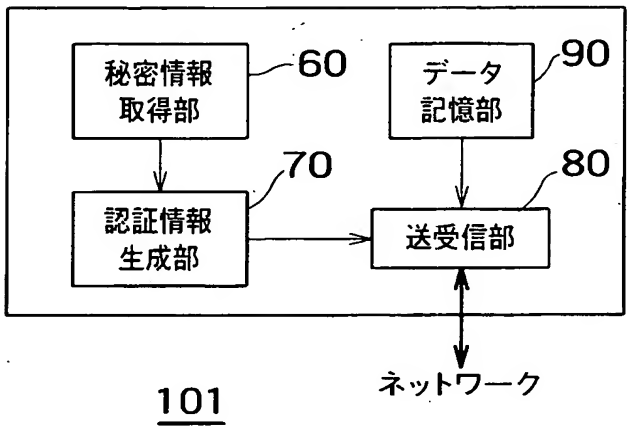
９４　送信データ生成部

【書類名】　図面

【図１】

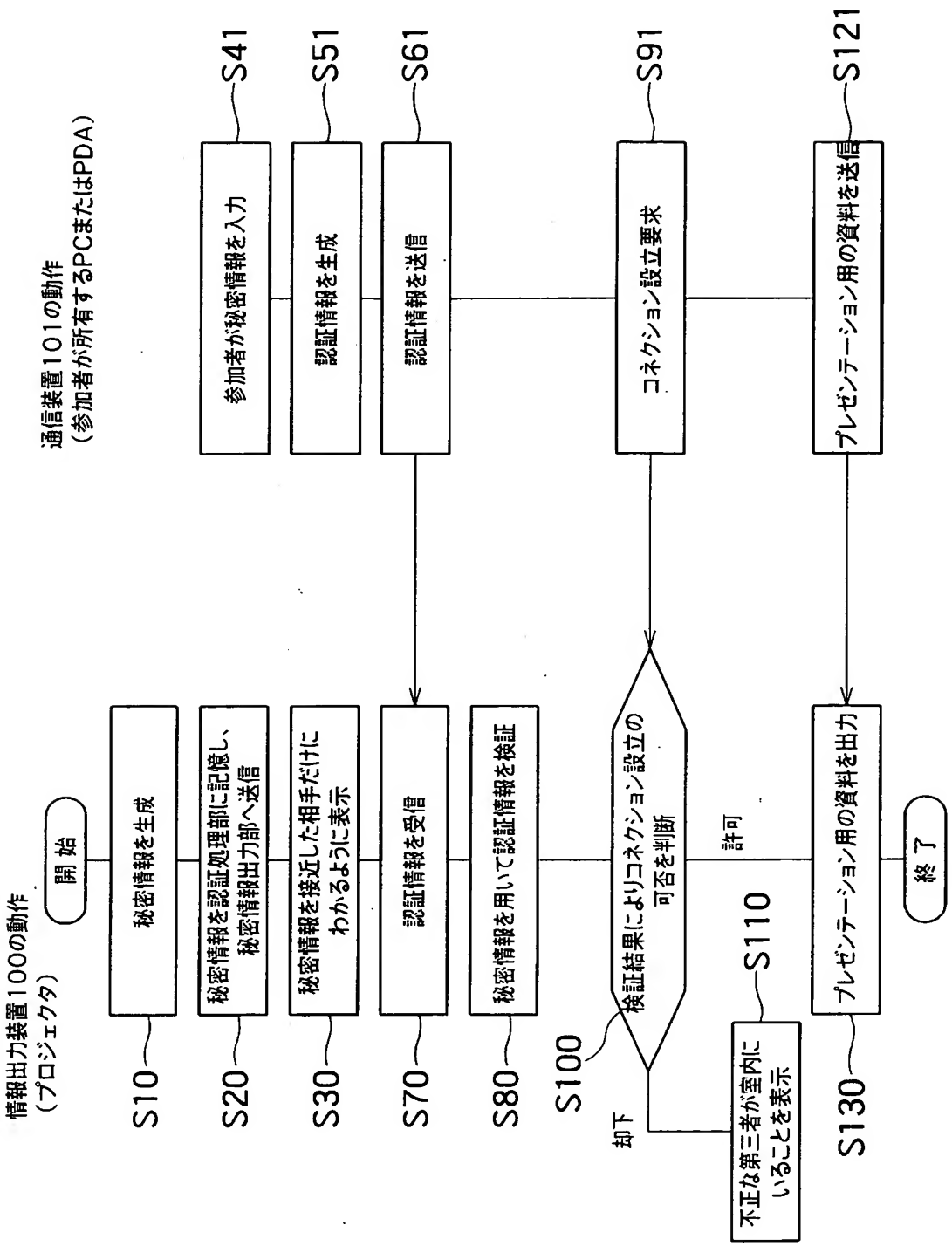

10
秘密情報
生成部
20
秘密情報
出力部
データ
出力部
50
40
認証処理部
30
送受信部
ネットワーク
100

（A）

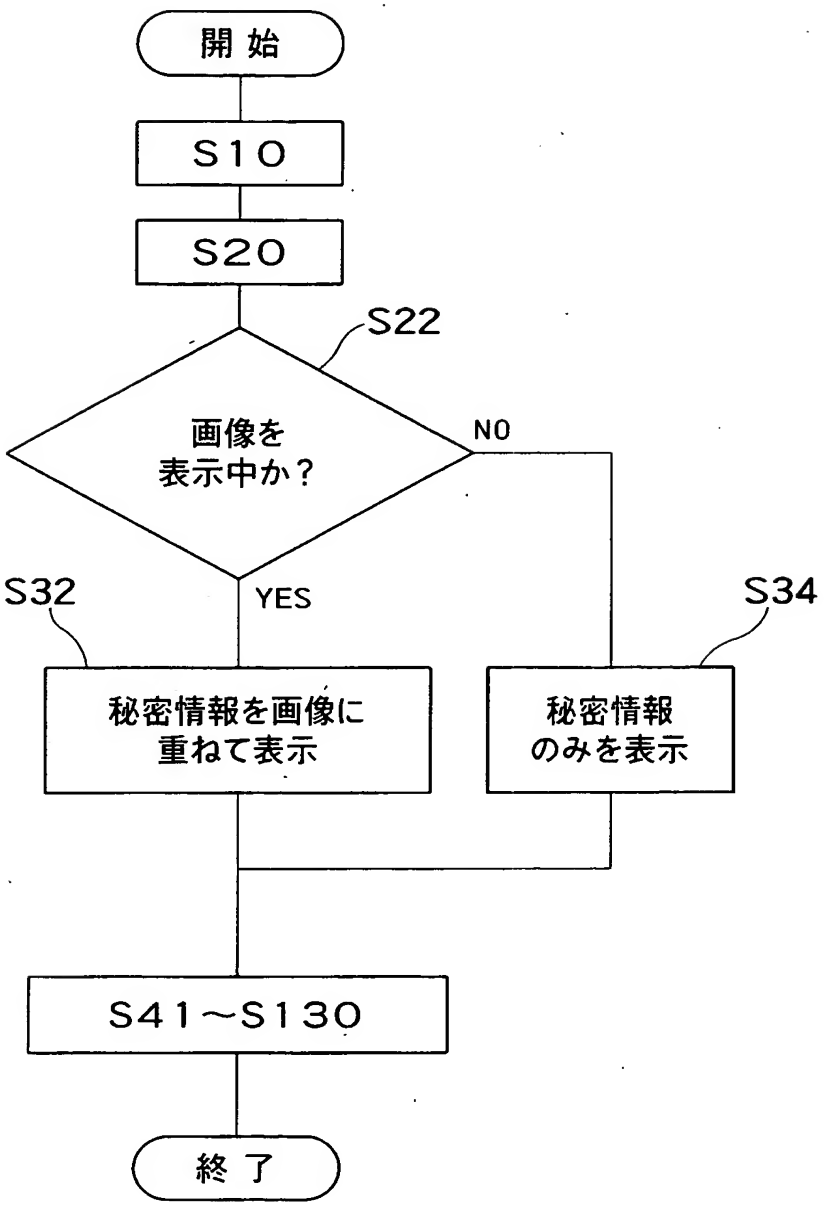

秘密情報
取得部
60
データ
記憶部
90
70
認証情報
生成部
80
送受信部
ネットワーク
101

（B）

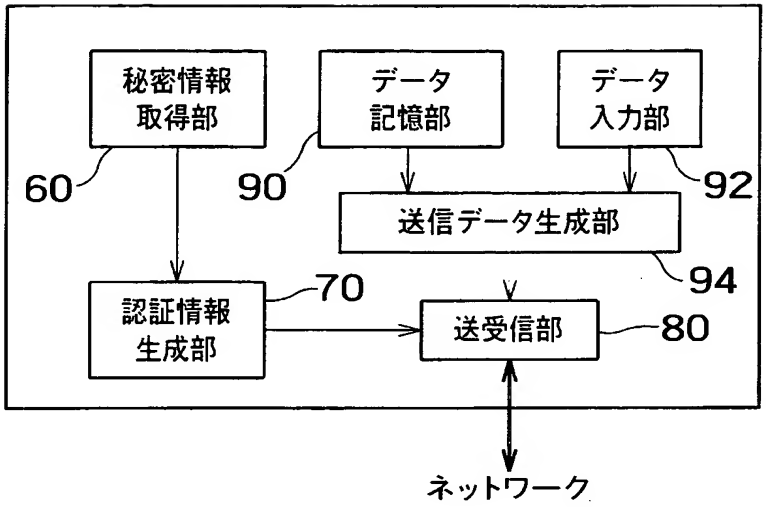
【図２】


情報出力装置100の動作
（プロジェクタ）
通信装置101の動作
（参加者が所有するPCまたはPDA）
開始
秘密情報を生成
S10
秘密情報を認証処理部に記憶し、
秘密情報出力部へ送信
S20
秘密情報を接近した相手だけに
わかるように表示
S30
認証情報を受信
S70
秘密情報を用いて認証情報を検証
S80
検証結果によりコネクション設立の
可否を判断
S100
却下
不正な第三者が室内に
いることを表示
S110
許可
プレゼンテーション用の資料を出力
S130
終了
参加者が秘密情報を入力
S41
認証情報を生成
S51
認証情報を送信
S61
コネクション設立要求
S91
プレゼンテーション用の資料を送信
S121

【図３】

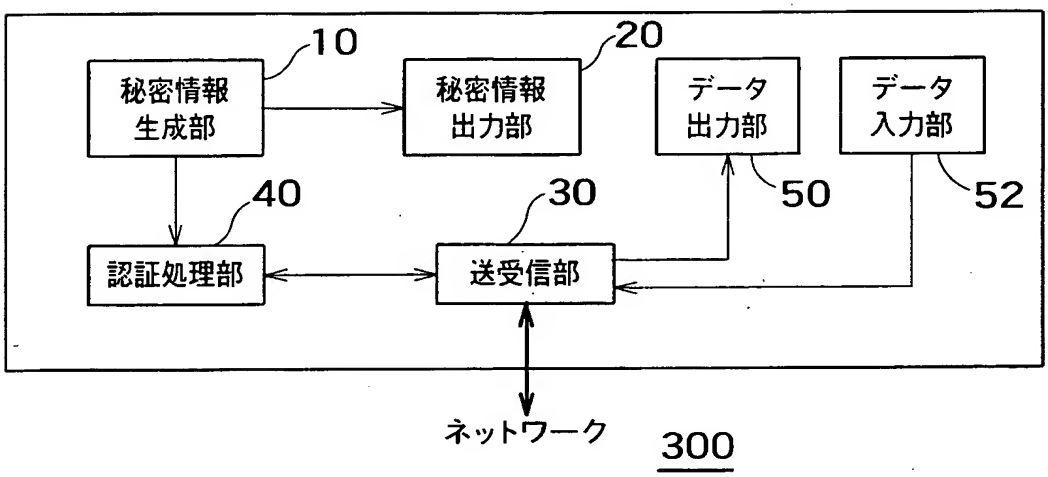

開 始
S10
S20
S22
画像を
表示中か？
NO
YES
S32
S34
秘密情報を画像に
重ねて表示
秘密情報
のみを表示
S41～S130
終 了

【図４】

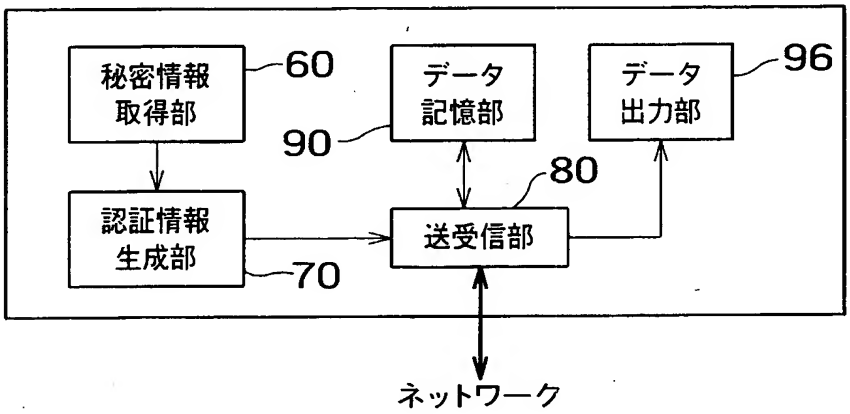

秘密情報
取得部
データ
記憶部
データ
入力部
60
90
92
送信データ生成部
94
認証情報
生成部
70
送受信部
80
ネットワーク

201

【図５】

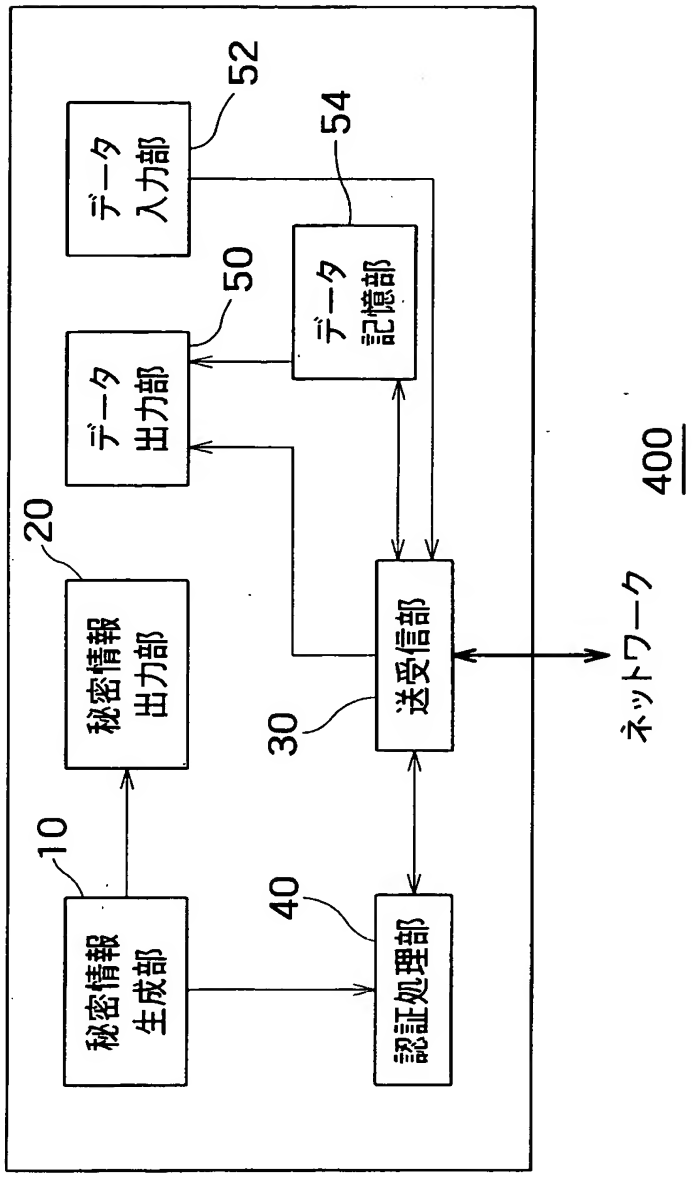

秘密情報
生成部
10
秘密情報
出力部
20
データ
出力部
50
データ
入力部
52
認証処理部
40
送受信部
30
ネットワーク
300

（A）

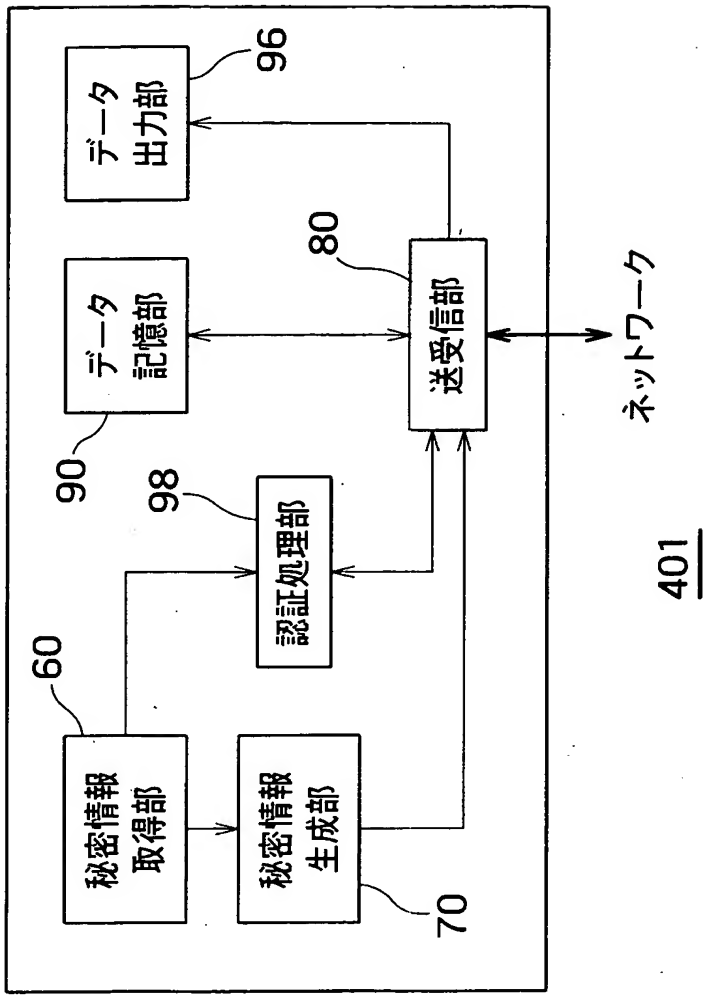

秘密情報
取得部
60
データ
記憶部
90
データ
出力部
96
認証情報
生成部
70
送受信部
80
ネットワーク
301

（B）

【図６】


400
ネットワーク
送受信部
30
データ入力部
52
データ記憶部
54
データ出力部
50
秘密情報出力部
20
秘密情報生成部
10
認証処理部
40

【図７】


データ出力部
96
データ記憶部
90
80
送受信部
ネットワーク
98
認証処理部
60
秘密情報取得部
秘密情報生成部
70
401

【書類名】　要約書

【要約】

【課題】　会議等の参加者以外の第三者による発表の妨害を防止し、参加者以外の第三者による発表内容の盗取を防止する情報表示装置、情報表示方法および情報表示システムを提供する。

【解決手段】　情報出力装置１００は、会議またはイベントの参加者が所有する通信装置１０１と無線通信可能な発表用の情報出力装置１００において、秘密情報を生成する秘密情報生成部１０と、通信装置１０１または参加者に対してのみ認識可能なように秘密情報を出力する秘密情報出力部２０と、秘密情報を入力した通信装置が該秘密情報に基づいて生成した認証情報を、該通信装置から受信する受信部３０と、秘密情報を用いて認証情報を検証することにより通信装置の認証を行う認証処理部４０とを備え、認証処理部により認証された通信装置が送信した発表情報を出力し、認証処理部により認証されていない通信装置が送信した発表情報を出力しない。

【選択図】　図１

特願２００３－０４７１２２

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝